Prefixes of minimal factorisations of a cycle

Thierry Lévy

PREFIXES OF MINIMAL FACTORISATIONS OF A CYCLE

THIERRY LÉVY

Abstract. We give a bijective proof of the fact that the number of k-prefixes of minimal factorisations of the n-cycle $(1 \dots n)$ as a product of $n-1$ transpositions is $n^{k-1}\binom{n}{k+1}$. Rather than a bijection, we construct a surjection with fibres of constant size. This surjection is inspired by a bijection exhibited by Stanley between minimal factorisations of an n-cycle and parking functions, and by a counting argument for parking functions due to Pollak.

1. Introduction

It is very well known that the n-cycle $(1 \dots n)$ cannot be written as a product of less than $n-1$ transpositions, and that there are n^{n-2} ways of writing it as a product of exactly $n-1$ transpositions. Among other proofs, the one given by R. Stanley in [5] relies on a bijection between minimal factorisations of $(1 \dots n)$ and parking functions of length $n-1$. The bijection is straightforward in one direction, from factorisations to parking functions, and more complicated in the other, but parking functions are very easily counted, thanks to a cunning argument which Stanley attributes to Pollak.

In [2], P. Biane generalised this result and proved that if $a_1, \dots, a_k$ are integers at least equal to 2 such that $(a_1 - 1) + \dots + (a_k - 1) = n - 1$, then there are n^{k-1} ways of writing the n-cycle $(1 \dots n)$ as a product $c_1 \dots c_k$ where c_i is an a_i-cycle for all $i \in [\![1, k]\!]$.

In this paper, we generalise the result in another direction by counting the initial segments of length $k \in [\![0, n-1]\!]$ of minimal factorisations of $(1 \dots n)$ by transpositions (see (1) for a precise definition). The number of these prefixes appears in the computation of the repartition of the eigenvalues of a large random unitary matrix taken under the heat kernel measure (see [3]). Using the deep relations between the unitary groups and the symmetric groups, it is possible to make these number appear under their combinatorial definition in this computation, and it is then crucial to be able to determine their value. This was done in [3], where it was proved that the number of these segments is $n^{k-1}\binom{n}{k+1}$. However, the proof given there was rather obscure and the goal of the present paper is to give a bijective proof of this identity.

The present proof consists in constructing a surjective mapping from the set $[\![1, n]\!]^k \times \binom{[\![1,n]\!]}{k+1}$ to the set of k-prefixes of minimal factorisations, with the property that the fibres of this surjection are exactly the orbits of the shift modulo n.

The paper is organised as follows. In Section 2, we describe the set which we want to enumerate and recall some classical facts about the geometry of the Cayley graph of the symmetric group. As a guide and motivation, we also give an informal description of the surjection. In Section 3, we collect various elementary properties of the prefixes of minimal factorisations of an n-cycle, in particular those for which the sequence of the smallest terms displaced by each successive transposition is non-decreasing. In Section 4, we describe an action of the symmetric group of order k on the set k-prefixes of minimal factorisations which plays a crucial role in the construction of the surjection. This construction is finally presented in Section 5, together with the study of the surjection and the proof of our counting result.

Date: May 29, 2011.

2. The Cayley graph of the symmetric group

The beginning of this section is meant to set up the notation and describe the problem. To start with, given two integers k and l such that $k < l$, we denote by $[\![k, l]\!]$ the set of integers $\{k, k+1, \ldots, l\}$.

Let $n \geq 1$ be an integer. Let $\mathfrak{S}_n$ be the symmetric group of order n. Let $\mathsf{T}_n \subset \mathfrak{S}_n$ be the subset which consists of all transpositions. It is a conjugacy class of $\mathfrak{S}_n$ and the Cayley graph of the pair $(\mathfrak{S}_n, \mathsf{T}_n)$ is defined without ambiguity regarding the order of multiplications. In this note, we endow $\mathfrak{S}_n$ with the graph distance of this Cayley graph.

This distance can be computed easily by counting the number of cycles of permutations. For all $\sigma \in \mathfrak{S}_n$, we denote by $\ell(\sigma)$ the number of cycles of σ, including the trivial cycles. For example, σ is a transposition if and only if $\ell(\sigma) = n-1$. The distance between two permutations σ_1 and σ_2 is simply $n - \ell(\sigma_1\sigma_2^{-1})$. We denote by $|\sigma|$ the number $n - \ell(\sigma)$. Note that for all permutation σ, one has $|\sigma^{-1}| = |\sigma|$.

The distance on $\mathfrak{S}_n$ allows one to define a partial order on $\mathfrak{S}_n$, by setting $\sigma_1 \preccurlyeq \sigma_2$ if and only if $|\sigma_2| = |\sigma_1| + |\sigma_1^{-1}\sigma_2|$. We are interested in computing the number of elements of the following set, defined for all $k \geq 0$:

$$\Sigma_n(k) = \Big\{(\tau_1, \ldots, \tau_k) \in (\mathsf{T}_n)^k : |\tau_1 \ldots \tau_k| = k,\ \tau_1 \ldots \tau_k \preccurlyeq (1 \ldots n)\Big\}. \tag{1}$$

We will see the elements $\Sigma_n(k)$ as paths in the symmetric group, according to the following convention : if $\gamma = (\tau_1, \ldots, \tau_k)$ is an element of $\Sigma_n(k)$, we denote for all $l \in [\![0, k]\!]$ by γ_l the permutation $\tau_1 \ldots \tau_l$. In particular, γ_0 is the identity.

The condition $|\tau_1 \ldots \tau_k| = k$ in the definition of $\Sigma_n(k)$ means that for each $l \in [\![1, k]\!]$, the multiplication on the right by τ_l reduces by 1 the number of cycles of the permutation $\tau_1 \ldots \tau_{l-1}$. This is equivalent to saying that the two elements of $[\![1, n]\!]$ which are exchanged by τ_l belong to distinct cycles of $\tau_1 \ldots \tau_{l-1}$.

The condition $\tau_1 \ldots \tau_k \preccurlyeq (1 \ldots n)$ means, according to the definition of the partial order, that the chain $(\tau_1, \ldots, \tau_k)$ of transpositions can be completed into a minimal factorisation of $(1 \ldots n)$, that is, a chain $(\tau_1, \ldots, \tau_{n-1}) \in (\mathsf{T}_n)^{n-1}$ such that $\tau_1 \ldots \tau_{n-1} = (1 \ldots n)$, or yet in other words, a shortest path from the identity to $(1 \ldots n)$.

From this description, it follows that $\Sigma_n(k)$ is

- empty if $k \geq n$,
- the set of minimal factorisations of $(1 \ldots n)$ if $k = n-1$,
- the projection of $\Sigma_n(n-1)$ on the first k coordinates of $(\mathsf{T}_n)^{n-1}$ if $k \leq n-1$.

In particular, if $(\tau_1, \ldots, \tau_k)$ belongs to $\Sigma_n(k)$, then $\tau_1 \ldots \tau_l \preccurlyeq (1 \ldots n)$ for all $l \in [\![0, k]\!]$. The following classical lemma enables us to decide when a permutation σ satisfies $\sigma \preccurlyeq (1 \ldots n)$.

Lemma 2.1. *Let $\sigma \in \mathfrak{S}_n$ be a permutation. The relation $\sigma \preccurlyeq (1 \ldots n)$ holds if and only if the following two conditions hold:*

1. *Each cycle of σ has the cyclic order induced by $(1 \ldots n)$.*
2. *The partition of $\{1, \ldots, n\}$ by the cycles of σ is non-crossing with respect to the cyclic order defined by $(1 \ldots n)$.*

The first condition is equivalent to the following: each cycle of σ can be written $(i_1 \ldots i_r)$ with $i_1 < \ldots < i_r$. The second condition means that there exist no subset $\{i, j, k, l\}$ of $[\![1, n]\!]$ with $i < j < k < l$ such that i and k belong to a cycle of σ and j and l belong to another cycle of σ.

It is well known that $\Sigma_n(n-1)$ has n^{n-2} elements. On the other extreme, $\Sigma_n(0)$ consists in the empty path and $\Sigma_n(1) = \mathsf{T}_n$ has $\binom{n}{2}$ elements. Our main goal is to give a bijective proof of the equality

$$|\Sigma_n(k)| = n^{k-1}\binom{n}{k+1}, \tag{2}$$

by the means of a surjective mapping

$$[\![1,n]\!]^k \times \binom{[\![1,n]\!]}{k+1} \to \Sigma_n(k),$$

such that the preimage of each element of $\Sigma_n(k)$ consists in n elements. In order to construct and study this mapping, we will need to get fairly concretely into the structure of the elements of $\Sigma_n(k)$ and this is what we begin in the next section. Before this, let us describe informally the surjection.

Let us start with a sequence $(a_1,\dots,a_k) \in [\![1,n]\!]^k$ and a subset $\{b_1,\dots,b_{k+1}\} \subset [\![1,n]\!]$. Let us reorder $(a_1,\dots,a_k)$ into a non-decreasing sequence $(i_1 \le \dots \le i_k)$. Consider a circular bike shed with n spaces labelled from 1 to n counterclockwise in the natural order, and in which only the spaces labelled $\{b_1,\dots,b_{k+1}\}$ are open. A first cyclist enters the shed just after the space i_k, expores the shed counterclockwise, thus starting from space i_k+1, and parks into the first open and available space. We denote this space by j_k. Then, $k-1$ other cyclists park one after the other, starting respectively just after the spaces $i_{k-1},\dots,i_1$. We record the spaces which they occupy as $j_{k-1},\dots,j_1$. At the end of the process, there is exactly one space left vacant among the $k+1$ open ones. If this space is not labelled by 1, we consider that the procedure has failed and we redo it from the beginning after applying to $(a_1,\dots,a_k)$ and $\{b_1,\dots,b_{k+1}\}$ the unique shift modulo n which ensures that the second attempt will not fail. We assume now that our initial data is such that the procedure does not fail.

Since the space 1 has not been occupied, no cyclist has gone past it in the process and the inequalities $i_1 < j_1,\dots,i_k < j_k$ hold. Moreover, we shall prove that $((i_1\,j_1),\dots,(i_k\,j_k))$ belongs to $\Sigma_n(k)$ (see Lemma 5.3).

Now, let $\sigma \in \mathfrak{S}_k$ be a permutation such that $(a_1,\dots,a_k) = (i_{\sigma(1)},\dots,i_{\sigma(k)})$. Let us emphasize that if the first attempt of our parking procedure failed, the sequences which we are considering here are those which we obtained after the shift. This permutation is not unique in general, but we shall prove that the result of the construction is independent of our choice (see Proposition 4.2). We want to let σ act on the path $((i_1\,j_1),\dots,(i_k\,j_k))$. For this, write σ as a product of transpositions of the form $(l\,l+1)$ with $l \in [\![1,k-1]\!]$ and let these transpositions act successively on $((i_1\,j_1),\dots,(i_k\,j_k))$ as follows: if $i_l = i_{l+1}$, do nothing, but if $i_l \neq i_{l+1}$, exchange $(i_l\,j_l)$ and $(i_{l+1}\,j_{l+1})$ and conjugate the one with the smallest i by the other.

Let us illustrate this on an example. Take $n=8$, $k=4$, consider the sequence $(1,3,7,1)$ and the subset $\{1,3,5,6,7\}$. The bikes enter the shed just after the spaces $7,3,1,1$ in this order and park respectively in the spaces $1,5,3,6$ (see Figure 1 below).

The procedure fails : the empty space is labelled 7. We must shift everything by 2 modulo 8 and redo the parking. The new sequence is $(3,5,1,3)$, the new subset $\{1,3,5,7,8\}$. The bikes enter the shed after the spaces $(5,3,3,1)$ and park at $(7,5,8,3)$. We obtain the chain $((1\,3),(3\,8),(3\,5),(5\,7))$. A permutation which transforms $(3,5,1,3)$ into $(1,3,3,5)$ is $(1\,3)(2\,4) = (2\,3)(1\,2)(3\,4)(2\,3)$. The transposition $(2\,3)$ does not change the chain, then $(3\,4)$ changes it to $((1\,3),(3\,8),(5\,7),(3\,7))$, then $(1\,2)$ to $((3\,8),(1\,8),(5\,7),(3\,7))$ and finally $(2\,3)$ to $((3\,8),(5\,7),(1\,8),(3\,7))$. This is the element of $\Sigma_8(4)$ which the surjection produces. It is indeed an element of $\Sigma_8(4)$, since $(3\,8)(5\,7)(1\,8)(3\,7) = (13578) \preccurlyeq (1\dots8)$ and $|(13578)| = 4$.

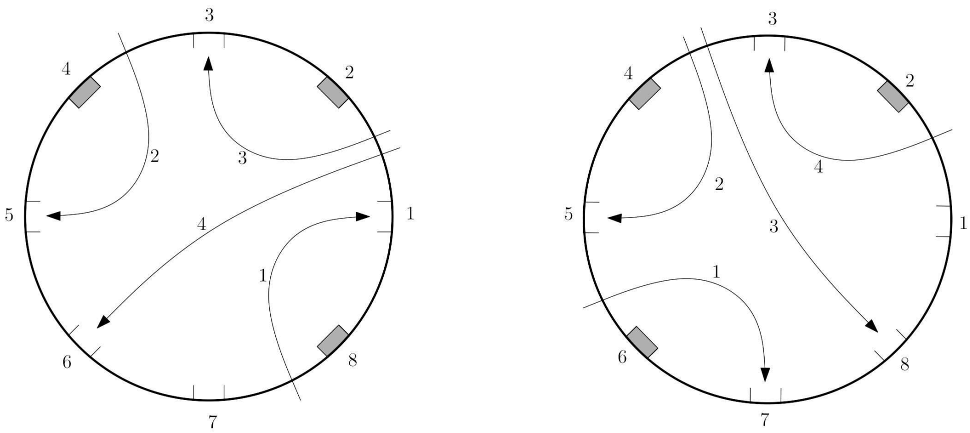

FIGURE 1. The paths of the bikes are labelled by their order of entrance in the shed. On the left-hand side, the original situation. On the right-hand side, the shifted one so that the space left vacant is 1. Observe that the order of entrance has been modified by the shift.

3. Non-decreasing geodesic paths

Let us agree on the convention that every time we write a transposition under the form $(i\,j)$, we mean $i < j$.

For all permutation $\pi \in \mathfrak{S}_n$ and all $x \in [\![1, n]\!]$, we denote by $C_\pi(x)$ the cycle of π which contains x. We will sometimes forget the cyclic order on $C_\pi(x)$ and consider it merely as a subset of $[\![1, n]\!]$. The following result is largely inspired by the proof of Theorem 3.1 in the work [5] of R. Stanley.

Lemma 3.1. *Let $\gamma = ((i_1\,j_1), \ldots, (i_k\;\,j_k))$ be an element of $\Sigma_n(k)$. Choose $l \in [\![1, k]\!]$. The following properties hold.*

1. $i_l < C_{\gamma_{l-1}}(j_l)$ and i_l is the largest element of $C_{\gamma_{l-1}}(i_l)$ with this property.
2. $j_l = \max C_{\gamma_{l-1}}(j_l)$.
3. $i_l < C_{\gamma_{l-1}}(i_l + 1)$.
4. If $i_l + 1 \notin \{i_1, i_2, \ldots, i_{l-1}\}$, then $C_{\gamma_{l-1}}(i_l + 1) = \{i_l + 1\}$.
5. If $k = n - 1$, $i_l = \max\{i_1, i_2, \ldots, i_{n-1}\}$ and $l = \max\{s \in [\![1, k]\!] : i_s = i_l\}$, then $j_l = i_l + 1$.

Proof. Since $|\gamma_l| = |\gamma_{l-1}| + 1$, i_l and j_l belong to distinct cycles of γ_{l-1} and to the same cycle of γ_l. The cycle of γ_l which contains i_l and j_l has the cyclic order induced by $(1 \ldots n)$, so that it is of the form $(x_1 < \ldots < x_r < i_l < y_1 < \ldots < y_s < j_l < z_1 < \ldots < z_t)$. The cycles of γ_{l-1} which contain i_l and j_l are thus respectively $(x_1 \ldots x_r\; i_l\; z_1 \ldots z_t)$ and $(y_1 \ldots y_s\; j_l)$. This proves the first two assertions.

The second part of the first assertion implies that $i_l + 1 \notin C_{\gamma_{l-1}}(i_l)$. If $i_l + 1 \in C_{\gamma_{l-1}}(j_l)$, then third assertion follows from the first. Let us assume that $i_l + 1 \notin C_{\gamma_{l-1}}(j_l)$. In this case, $C_{\gamma_{l-1}}(i_l + 1) = C_{\gamma_l}(i_l + 1)$. Suppose that there is an element x in $C_{\gamma_{l-1}}(i_l + 1)$ such that $x < i_l$. Then the quadruplet $x < i_l < i_l + 1 < y_l$ would violate the non-crossing condition on the cycles of γ_l imposed by the condition $\gamma_l \preccurlyeq (1 \ldots n)$. This concludes the proof of the third assertion.

Let us assume that $i_l + 1 \notin \{i_1, \ldots, i_{l-1}\}$. Let r be the smallest element of $[\![1, k]\!]$, if it exists, such that the cycle of $i_l + 1$ in γ_r is not reduced to the singleton $\{i_l + 1\}$. We must have $i_r = i_l + 1$ or $j_r = i_l + 1$. If $i_r = i_l + 1$, then our assumption implies $r \geq l$, so that $C_{\gamma_{l-1}}(i_l + 1) = \{i_l + 1\}$. If $j_r = i_l + 1$, then $i_r \in C_{\gamma_r}(i_l + 1)$. Since $i_r \leq i_l$ and thanks to the third assertion, this implies that $r \geq l$, so that in this case also we have $C_{\gamma_{l-1}}(i_l+1) = \{i_l+1\}$. This proves the fourth assertion.

Let us assume that $k = n-1$, $i_l = \max\{i_1, i_2, \dots, i_{n-1}\}$ and $l = \max\{s \in [\![1,k]\!] : i_s = i_l\}$. We are thus looking, in a minimal factorisation of $(1\dots n)$, at the last occurrence of the largest i. Let, as before, r be the smallest element of $[\![1,n-1]\!]$ such that $C_{\gamma_r}(i_l+1)$ is not reduced to the singleton $\{i_l+1\}$. Since $(1\dots n)$ has no fixed point, we know for sure that r exists. By maximality of i_l, we have $i_l+1 = j_r$. If $r > l$, then by maximality of i_l and of l, we have $i_r < i_l$. Thus, the quadruplet $i_r < i_l < i_l+1 < j_l$ violates the non-crossing condition on the cycles of the permutation γ_r. This proves the fifth assertion. $\square$

We now make an observation of monotonicity.

Lemma 3.2. *Consider $\gamma = ((i_1\, j_1), \dots, (i_k\, j_k)) \in \Sigma_n(k)$ and $l, m \in [\![1,k]\!]$ with $l < m$.*
1. If $i_l = i_m$, then $j_l > j_m$.
2. If $j_l = j_m$, then $i_l > i_m$.

Proof. Let us assume that $i_l = i_m$. We have $j_m \notin C_{\gamma_{m-1}}(i_m)$ and $j_l \in C_{\gamma_{m-1}}(i_l) = C_{\gamma_{m-1}}(i_m)$. In particular, $j_l \neq j_m$. Both i_m and j_l belong to $C_{\gamma_{m-1}}(i_m)$ but, according to the first assertion of Lemma 3.1, i_m is the largest element of $C_{\gamma_{m-1}}(i_m)$ which is smaller than any element of $C_{\gamma_{m-1}}(j_m)$. Hence, there exists $x \in C_{\gamma_{m-1}}(j_m)$ such that $i_m = i_l < x < j_l$. The inequality $j_l < j_m$ cannot hold, for then the quadruplet $i_l < x < j_l < j_m$ would violate the non-crossing property of the cycles of γ_{m-1}.

The second assertion follows from the first and the existence of a simple involution of $\Sigma_n(k)$, which we describe in Lemma 3.3 below. $\square$

Lemma 3.3. *Let $((i_1\, j_1), \dots, (i_k\, j_k))$ be an element of $\Sigma_n(k)$. Then the chain of transpositions $((n+1-j_k\; n+1-i_k), \dots, (n+1-j_1\; n+1-i_1))$ is also an element of $\Sigma_n(k)$.*

Proof. Let $\varphi \in \mathfrak{S}_n$ be the involution which exchanges i and $n+1-i$ for all $i \in \{1, \dots, n\}$. The point is the identity $\varphi(1\dots n)^{-1}\varphi^{-1} = (1\dots n)$. Let $(\tau_1, \dots, \tau_k)$ be an element of $\Sigma_n(k)$. Then on one hand $|\varphi\tau_k \dots \tau_1\varphi^{-1}| = |\tau_k \dots \tau_1| = |\tau_1 \dots \tau_k| = k$. On the other hand, we have the equality $|(1\dots n)^{-1}\varphi\tau_k \dots \tau_1\varphi^{-1}| = |\varphi^{-1}(1\dots n)^{-1}\varphi\tau_k \dots \tau_1| = |(1\dots n)(\tau_1 \dots \tau_k)^{-1}| = n-1-k$. Hence, $\varphi\tau_k \dots \tau_1\varphi^{-1} \preccurlyeq (1\dots n)$. Finally, $(\varphi\tau_k\varphi^{-1}, \dots, \varphi\tau_1\varphi^{-1})$ belongs to $\Sigma_n(k)$. $\square$

It turns out that the elements of $\Sigma_n(k)$ for which the sequence $(i_1, \dots, i_n)$ is non-decreasing are easy to describe and to characterise. We call them *non-decreasing paths* and we denote by $\Sigma_n^*(k)$ the subset of $\Sigma_n(k)$ which they constitute.

Lemma 3.4. *Let $\gamma = ((i_1\, j_1), \dots, (i_k\; j_k))$ be an element of $\Sigma_n^*(k)$. The following properties hold.*
1. The sequence $(j_1, \dots, j_k)$ has no repetitions.
2. For all $l \in [\![1,k]\!]$, j_l is a fixed point of γ_{l-1}.
3. For all $l \in [\![1,k]\!]$, γ_l is obtained from γ_{l-1} by inserting j_l into the cycle of i_l immediately after i_l.
4. For all $m \in [\![1,k]\!]$, the support of γ_m is $\bigcup_{l=1}^m \{i_l\} \cup \{j_l\}$.

Proof. The second assertion of Lemma 3.2 implies that each repetition in the sequence $(j_1, \dots, j_k)$ corresponds to a descent in the sequence $(i_1, \dots, i_k)$, hence the first assertion.

For all $l \in [\![1,k]\!]$, we have $j_l > i_l \geq \ldots \geq i_1$ and, by the first assertion, $j_l \notin \{j_1, \dots, j_{l-1}\}$, so that j_l is a fixed point of γ_{l-1}. This is the second assertion.

For all $l \in [\![1,k]\!]$, the second assertion implies that $\gamma_l(i_l) = j_l$, and we have $\gamma_l(j_l) = \gamma_{l-1}(i_l)$. This is exactly the third assertion.

The fourth assertion follows from the second and third assertions by induction on k. $\square$

Proposition 3.5. *Consider $((i_1\, j_1), \ldots, (i_k\, j_k)) \in (\mathsf{T}_n)^k$. Assume that $i_1 \le \ldots \le i_k$. The following properties are equivalent.*

1. $((i_1\, j_1), \ldots, (i_k\, j_k)) \in \Sigma_n(k)$.
2. For all $l, m \in \{1, \ldots, n-1\}$ such that $l < m$, one either has $j_l \le i_m$ or $j_l > j_m$.

Proof. Let us prove that the first property implies the second. For this, let us choose $\gamma = ((i_1\, j_1), \ldots, (i_k\, j_k)) \in \Sigma_n(k)$ and l, m with $1 \le l < m \le n-1$. It follows from the first assertion of Lemma 3.4 that $j_l \neq j_m$. Let us assume by contradiction that $i_m < j_l < j_m$. Then, by Lemma 3.2, $i_l < i_m$. Hence, $i_l < i_m < j_l < j_m$. We know, by the second assertion of Lemma 3.4, that $C_{\gamma_{m-1}}(j_m) = \{j_m\}$. We claim that $i_m \notin C_{\gamma_{m-1}}(i_l)$. Otherwise, since $j_l \in C_{\gamma_{m-1}}(i_l)$, the element j_l of $C_{\gamma_{m-1}}(i_m)$ would satisfy both $j_l > i_m$ and $j_l < C_{\gamma_{m-1}}(j_m)$, in contradiction with the first assertion of Lemma 3.1.

It follows from this argument that neither i_m nor j_m belong to the common cycle of i_l and j_l in γ_{m-1}. Hence, the two cycles $C_{\gamma_m}(i_l) = C_{\gamma_m}(j_l)$ and $C_{\gamma_m}(i_m) = C_{\gamma_m}(j_m)$ are distinct. Since $i_l < i_m < j_l < j_m$, this contradicts the non-crossing property of the cycles of γ_m.

Let us now prove that the second property implies the first. To start with, observe that the second property implies that $j_1, \ldots, j_k$ are pairwise distinct and that the equality $i_l = i_m$ for $l < m$ implies $j_l > j_m$.

We now proceed by induction on k. If $k = 1$, then the result is true because $\Sigma_n(1) = \mathsf{T}_n$. Let us assume that the result holds for paths of length up to $k-1$ and let us consider a path $\gamma = ((i_1\, j_1), \ldots, (i_k\, j_k)) \in (\mathsf{T}_n)^k$ such that $i_1 \le \ldots \le i_k$ and the second property holds. By induction, γ_{k-1} is a product of $n-k+1$ cycles with the cyclic order induced by $(1 \ldots n)$ and which form a non-crossing partition of $\{1, \ldots, n\}$.

By the third assertion of Lemma 3.4, γ_k a product of $n-k$ cycles.

Let us prove that the cyclic order of the new cycle is the order induced by $(1 \ldots n)$. We certainly have $i_k < j_k$ and we claim that $i_k < j_k < \gamma_{k-1}(i_k)$ in the cyclic order of $(1 \ldots n)$, which means exactly that $\gamma_{k-1}(i_k) \le i_k$ or $\gamma_{k-1}(i_k) > j_k$. But $\gamma_{k-1}(i_k)$ is either i_l for some $l \in [\![1, k-1]\!]$, in which case $\gamma_{k-1}(i_k) \le i_k$, or $\gamma_{k-1}(i_k)$ is j_l for some $l \in [\![1, k-1]\!]$, in which case $\gamma_{k-1}(i_k) \le i_k$ or $\gamma_{k-1}(i_k) > j_k$, by the main assumption.

Let us finally prove that the cycles of γ_k form a non-crossing partition. The only way this could not be true is if some cycle contained two elements x and y such that $i_k < x < j_k < y < \gamma_{k-1}(i_k)$ in the cyclic order. But the any x such that $i_k < x < j_k$ does neither belong to $\{i_1, i_2, \ldots, i_k\}$ nor to $\{j_1, j_2, \ldots, j_k\}$ and hence is a fixed point of γ_k. □

This proposition allows us to prove that a non-decreasing path $\gamma \in \Sigma_n^*(k)$ is completely determined by the sequence $(i_1, \ldots, i_k)$ and the support of γ_k.

Corollary 3.6. *Let $\gamma = ((i_1\, j_1), \ldots, (i_k\, j_k))$ be an element of $\Sigma_n^*(k)$. For all $l \in [\![1, k]\!]$, j_l is the minimum of the intersection of $[\![i_l + 1, n]\!]$ with the support of γ_l.*

Moreover, if $\tilde{\gamma} = ((i_1\, \tilde{j}_1), \ldots, (i_k\, \tilde{j}_k))$ is another element of $\Sigma_n^*(k)$ such that $\tilde{\gamma}_k$ and γ_k have the same support, then $\tilde{\gamma} = \gamma$.

Proof. The support of γ_l is $\bigcup_{s=1}^{l} \{i_s\} \cup \{j_1, \ldots, j_l\}$. For all $s < l$, we have $i_s \le i_l$ and, by Proposition 3.5, $j_s \le i_l$ or $j_s > j_l$. The first assertion follows.

Let us prove the second assertion by induction on k. The result is true for $k = 0$. Let us assume that is has been proved for paths of length up to $k-1$. By the first assertion, $\tilde{j}_k = j_k$. Hence, $\delta = ((i_1\, j_1), \ldots, (i_{k-1}\, j_{k-1}))$ and $\tilde{\delta} = ((i_1\, \tilde{j}_1), \ldots, (i_{k-1}\, \tilde{j}_{k-1}))$ are two elements of $\Sigma_n(k-1)$ such that $\tilde{\delta}_{k-1}$ and δ_{k-1} have the same support. By induction, they are equal. □

4. Permutation of geodesic paths

In this section, we will describe an action of the group $\mathfrak{S}_k$ on $\Sigma_n(k)$. More precisely, let us consider the projection $P : \Sigma_n(k) \to [\![1, n-1]\!]^k$ which sends the chain $((i_1\, j_1), \ldots, (i_k\, j_k))$ to the sequence $(i_1, \ldots, i_k)$. The group $\mathfrak{S}_k$ acts naturally on $[\![1, n-1]\!]^k$ by the formula $\sigma \cdot (i_1, \ldots, i_k) = (i_{\sigma^{-1}(1)}, \ldots, i_{\sigma^{-1}(k)})$ and we will endow $\Sigma_n(k)$ with an action of $\mathfrak{S}_k$ such that P is an equivariant mapping which preserves the stabilisers. This last condition is equivalent to the fact that the restriction of P to each orbit of $\mathfrak{S}_k$ in $\Sigma_n(k)$ is an injection.

In order to define the action of $\mathfrak{S}_k$ on $\Sigma_n(k)$, we will use the classical action of the braid group B_k on the product of k copies of an arbitrary group G (see for example [1]). If $\beta_1, \ldots, \beta_k$ are the usual generators of B_k, this action is given by the formula

$$\beta_l \cdot (g_1, \ldots, g_k) = (g_1, \ldots, g_{l+1}, g_{l+1}^{-1} g_l g_{l+1}, \ldots, g_k),$$

valid for all $(g_1, \ldots, g_k) \in G^k$ and all $l \in [\![1, k-1]\!]$. Observe that if $T \subset G$ is a conjugacy class, then T^k is stable under this action. Moreover, the product map $(g_1, \ldots, g_n) \mapsto g_1 \ldots g_n$ is invariant under this action.

Let us denote by $\sigma_1 = (1\,2), \ldots, \sigma_{k-1} = (k-1\, k)$ the Coxeter generators of $\mathfrak{S}_k$, so that the natural mophism $B_k \to \mathfrak{S}_k$ sends β_l to σ_l for all $l \in [\![1, k-1]\!]$. Consider $\gamma = ((i_1\, j_1), \ldots, (i_k\, j_k))$ in $\Sigma_n(k)$ and $l \in [\![1, k-1]\!]$. Set

$$\sigma_l \cdot \gamma = \begin{cases} \gamma & \text{if } i_l = i_{l+1}, \\ \beta_l \cdot \gamma & \text{if } i_l < i_{l+1}, \\ \beta_l^{-1} \cdot \gamma & \text{if } i_l > i_{l+1}. \end{cases} \tag{3}$$

Since the action of the braid group preserves the ordered product of the components, $\sigma_l \cdot \gamma$ belongs to $\Sigma_n(k)$.

Practically, $\sigma_l \cdot \gamma$ is obtained from γ by doing nothing if $i_l = i_{l+1}$, and otherwise, by swapping the l-th and $(l+1)$-th elements of γ and conjugating the one with the smallest i by the other. In this way, the transposition with the largest i is not modified, and only the j of the other is affected. For example, if $k = 2$,

$$\begin{aligned} \sigma_1 \cdot ((1\,3), (1\,2)) &= ((1\,3), (1\,2)), \\ \sigma_1 \cdot ((1\,2), (2\,3)) &= ((2\,3), (1\,3)), \\ \sigma_1 \cdot ((2\,3), (1\,3)) &= ((1\,2), (2\,3)). \end{aligned}$$

A straightforward inspection will convince the reader of the following fact.

Lemma 4.1. *For all $\gamma \in \Sigma_n(k)$ and $l \in [\![1, k-1]\!]$, one has $P(\sigma_l \cdot \gamma) = \sigma_l \cdot P(\gamma)$.*

Moreover, if $\gamma = ((i_1\, j_1), \ldots, (i_k\, j_k))$ and $\sigma_l \cdot \gamma = ((i_{\sigma_l^{-1}(1)}\, \tilde{j}_1), \ldots, (i_{\sigma_l^{-1}(k)}\, \tilde{j}_k))$, then the sets $\bigcup_{l=1}^k \{i_l\} \cup \{j_l\}$ and $\bigcup_{l=1}^k \{i_l\} \cup \{\tilde{j}_l\}$ are equal.

We will show at the end of this section that the set $\bigcup_{l=1}^k \{i_l\} \cup \{j_l\}$ is the support of γ_k. For the time being, let us prove that (3) defines an action of $\mathfrak{S}_k$ on $\Sigma_n(k)$.

Proposition 4.2. *The action of the Coxeter generators of $\mathfrak{S}_k$ on $\Sigma_n(k)$ defined by (3) extends to an action of $\mathfrak{S}_k$.*

Moreover, the mapping $P : \Sigma_n(k) \to [\![1, n-1]\!]^k$ is equivariant and preserves the stabilisers : for all $\gamma \in \Sigma_n(k)$ and all $\pi \in \mathfrak{S}_k$, one has $\pi \cdot P(\gamma) = P(\gamma)$ if and only if $\pi \cdot \gamma = \gamma$.

Proof. We must prove that the operations which we have defined satisfy the Coxeter relations $\sigma_l^2 = \mathrm{id}$ for $l \in [\![1, k-1]\!]$, $(\sigma_l \sigma_m)^2 = \mathrm{id}$ for $l, m \in [\![1, k-1]\!]$ with $|l - m| \geq 2$, and $(\sigma_l \sigma_{l+1})^3 = \mathrm{id}$ for $l \in [\![1, n-2]\!]$.

The first relation follows from Lemma 4.1. Indeed, $\sigma_l \cdot (\sigma_l \cdot \gamma)$ is either γ or $\beta_l \beta_l^{-1} \cdot \gamma$ or $\beta_l^{-1}\beta_l \cdot \gamma$, hence in any case γ. The second relation is equivalent to $\sigma_l \cdot (\sigma_m \cdot \gamma) = \sigma_m \cdot (\sigma_l \cdot \gamma)$ and it clearly holds for $|l-m| \geq 2$. In order to prove the third relation, there are six cases to consider, correponding to the possible relative positions of i_l, i_{l+1} and i_{l+2}. In each case, the relation $\beta_l\beta_{l+1}\beta_l = \beta_{l+1}\beta_l\beta_{l+1}$ implies the relation $(\sigma_l\sigma_{l+1})^3 = \mathrm{id}$.

We have thus an action of the symmetric group $\mathfrak{S}_k$ on $\Sigma_n(k)$. By Lemma 4.1, the mapping P is equivariant under this action and the natural action on $[\![1, n-1]\!]^k$. If $\gamma \in \Sigma_n(k)$ and $\pi \in \mathfrak{S}_k$ satisfy $\pi \cdot \gamma = \gamma$, then $\pi \cdot P(\gamma) = P(\pi \cdot \gamma) = P(\gamma)$. Finally, let us prove that $\pi \cdot P(\gamma) = P(\gamma)$ implies $\pi \cdot \gamma = \gamma$. Let us choose $\gamma \in \Sigma_n(k)$. A permutation π stabilises $P(\gamma)$ if and only if its cycles are contained in the level sets of the mapping $1 \mapsto i_1, \ldots, k \mapsto i_k$. Thus, the stabiliser of $P(\gamma)$ is generated by the transpositions which it contains, and we may restrict ourselves to the case where π is a transposition $(l\,m)$ with $i_l = i_m$. We have $(l\,m) = \sigma_l \ldots \sigma_{m-2}\sigma_{m-1}\sigma_{m-2} \ldots \sigma_l$ and $\sigma_{m-2} \ldots \sigma_l = (m-1 \ldots l)$. Since P is equivariant, the transpositions which are at the positions $m-1$ and m in the chain $\sigma_{m-2} \ldots \sigma_l \cdot \gamma$ have respectively i_l and i_m as their smallest element. Since $i_l = i_m$, we find

$$(l\,m) \cdot \gamma = \sigma_l \ldots \sigma_{m-2}\sigma_{m-1}\sigma_{m-2} \ldots \sigma_l \cdot \gamma = \sigma_l \ldots \sigma_{m-2}\sigma_{m-2} \ldots \sigma_l \cdot \gamma = \gamma,$$

as expected. □

Corollary 4.3. *Let $\gamma = ((i_1\,j_1), \ldots, (i_k\,j_k))$ be an element of $\Sigma_n(k)$. The support of $\gamma_k = (i_1\,j_1) \ldots (i_k\,j_k)$ is the set $\bigcup_{l=1}^k \{i_l\} \cup \{j_l\}$.*

Proof. The action of $\mathfrak{S}_k$ on $\Sigma_n(k)$ preserves both the support of γ_k and the set to which we wish to show that it is equal. Since every orbit contains a non-decreasing chain, that is, a chain for which the sequence $(i_1, \ldots, i_n)$ is non-decreasing, we may assume that the element γ which we are considering has this property, and apply the fourth assertion of Lemma 3.4. □

In the context of minimal factorisations of a cycle, the natural action of the braid group is called the Hurwitz action and it is known to be transitive (see for example [4]). The action which we have defined here is germane to this action but different, as it is an action of the symmetric group. In [2], P. Biane defined yet another similar action of the symmetric group on minimal factorisations of a cycle as a product of cycles. The proof of Lemma 4.1 is inspired by this work.

5. The main surjection

We have now gathered the information necessary to define the surjection which is our main goal. Although we do not develop this point, our construction is inspired by the enumeration of parking functions by an argument due to Pollak, and the bijection constructed by Stanley between parking functions and minimal factorisations of an n-cycle (see [5]).

Let us start by formalising the parking process in a bike shed described in Section 2. Given a sequence $E = (e_1, \ldots, e_k) \in [\![1, n]\!]^k$ of entry points and a set $O = \{o_1, \ldots, o_{k+1}\} \subset [\![1, n]\!]$ of open spaces, we define a sequence of parking spaces $(p_1, \ldots, p_k)$ by backwards induction, by setting

$$p_k = (1 \ldots n)^r e_k, \text{ where } r = \min\{s \in [\![1, n]\!] : (1 \ldots n)^s e_k \in \{o_1, \ldots, o_{k+1}\}\} \tag{4}$$

and, assuming that $p_k, \ldots, p_{l+1}$ have been defined,

$$p_l = (1 \ldots n)^r e_l, \text{ where } r = \min\{s \in [\![1, n]\!] : (1 \ldots n)^s e_l \in \{o_1, \ldots, o_{k+1}\} \setminus \{p_{l+1}, \ldots, p_k\}\}. \tag{5}$$

We call this construction the parking process and write $\Pi(E, O) = (p_1, \ldots, p_k)$. The set $O \setminus \{p_1, \ldots, p_k\}$ consists of a single element, which we call the residue and denote by $\rho(E, O)$.

Let us state the properties of the parking process which matter for our construction. In what follows, we call shift modulo n the action of $\mathbb{Z}/n\mathbb{Z}$ on $[\![1,n]\!]^k$ and $\binom{[\![1,n]\!]}{k+1}$ determined componentwise and elementwise in the ovious way by the n-cycle $(1\dots n)$.

Lemma 5.1. *1. The parking process is equivariant with respect to the shift modulo n, that is, $\Pi((1\dots n)E,(1\dots n)O) = (1\dots n)\Pi(E,O)$ and $\rho((1\dots n)E,(1\dots n)O) = (1\dots n)\rho(E,O)$*
2. If E' differs from E by a permutation, then $\Pi(E',O)$ differs from $\Pi(E,O)$ by a permutation. In particular, $\rho(E',O) = \rho(E,O)$.
3. If $\rho(E,O) = 1$, then for all $l \in [\![1,k]\!]$, one has $e_l < p_l$.

Proof. The shift modulo n is an automorphism of the set $[\![1,n]\!]$ endowed with the cyclic order determined by $(1\dots n)$. The definition of the parking process by the equations (4) and (5) uses only this structure of cyclic order. Hence, the first assertion holds.

In order to check the second assertion, it suffices to check that the set $\{p_1,\dots,p_k\}$ is not modified by the permutation of two neighbours in the sequence E. This is a simple verification which we leave to the reader.

Let us assume that $\rho(E,O) = 1$. Then, for all $l \in [\![1,k]\!]$, the integer 1 belongs to $\{o_1,\dots,o_{k+1}\}\setminus\{p_{l+1},\dots,p_k\}$. Hence, the integer $r \in [\![1,n]\!]$ such that $p_l = (1\dots n)^r e_l$ satisfies $r \le n+1-e_l$, actually even $r < n+1-e_l$ because $p_l \neq 1$, so that $e_l < p_l \le n$. □

Let us now begin the construction of the surjection itself. Consider $A = (a_1,\dots,a_k) \in [\![1,n]\!]^k$ and $B = \{b_1,\dots,b_{k+1}\} \subset [\![1,n]\!]$. Let us apply to A and B the shift modulo n which ensures that the residue of the parking process applied to A and B is 1. Thus, let us define $\tilde{A} = (1\dots n)^{1-\rho(A,B)}A$ and $\tilde{B} = (1\dots n)^{1-\rho(A,B)}B$.

Let $I = (i_1 \le \dots \le i_k)$ be the non-decreasing reordering of $\tilde{A}$. Let $J = (j_1,\dots,j_k) = \Pi(I,\tilde{B})$ be the result of the parking process applied to I and $\tilde{B}$.

Lemma 5.2. *The inequalities $i_1 < j_1,\dots,i_k < j_k$ hold.*

Proof. By the first assertion of Lemma 5.1, we have $\rho(\tilde{A},\tilde{B}) = 1$. Since I differs from $\tilde{A}$ by a permutation, the second assertion of the same lemma implies that $\rho(I,\tilde{B}) = 1$. The third assertion of the same lemma concludes the proof. □

The main property of the construction so far is the following.

Lemma 5.3. *The chain $((i_1\, j_1),\dots,(i_k\, j_k))$ belongs to $\Sigma_n^*(k)$.*

Proof. Since the sequence $(i_1,\dots,i_k)$ is non-decreasing, it suffices to check that the second property of Proposition 3.5 is satisfied. Let us choose $l,m \in [\![1,k]\!]$ with $l < m$ and let us assume that $j_l > i_m$. We need to prove that $j_l > j_m$.

We have $j_m = \min\Big([\![i_m+1,n]\!] \cap (\{\tilde{b}_1,\dots,\tilde{b}_{k+1}\} \setminus \{j_{m+1},\dots,j_k\})\Big)$ and, since we are assuming that $j_l > i_m$, $j_l = \min\Big([\![i_m+1,n]\!] \cap (\{\tilde{b}_1,\dots,\tilde{b}_{k+1}\} \setminus \{j_{l+1},\dots,j_k\})\Big)$. Thus, j_l is the minimum of a set which is contained in another set of which j_m is the minimum. □

In order to complete the construction, let us choose a permutation $\sigma \in \mathfrak{S}_k$ such that $\sigma\cdot\tilde{A} = I$. There is in general more than one choice for σ, but two different choices belong to the same right coset of the stabilizer of I. Since the mapping P preserves the stabilisers (see Proposition 4.2), the element

$$\Gamma_{n,k}(A,B) = \sigma^{-1}\cdot((i_1\, j_1),\dots,(i_k\, j_k))$$

of $\Sigma_n(k)$ is well defined.

Theorem 5.4. *The mapping* $\Gamma_{n,k} : [\![1,n]\!]^k \times \binom{[\![1,n]\!]}{k+1} \to \Sigma_n(k)$ *is a surjection whose fibres are the orbits of the shift modulo* n*. In particular, the preimage of each element of* $\Sigma_n(k)$ *contains* n *elements and* $|\Sigma_n(k)| = n^{k-1}\binom{n}{k+1}$.

Proof. In order to prove that the mapping $\Gamma_{n,k}$ is surjective, let us construct a section of it.

Let $\gamma = ((i_1\, j_1), \ldots, (i_k\, j_k))$ be an element of $\Sigma_n(k)$. Let $\sigma \in \mathfrak{S}_k$ be a permutation such that $\sigma \cdot \gamma = ((a_1\, b_1), \ldots, (a_k\, b_k))$ satisfies $a_1 \leq \ldots \leq a_k$. Set $b_{k+1} = 1$. By Lemma 3.4, the set $\{b_1, \ldots, b_{k+1}\}$ contains $k+1$ elements. Proposition 3.5 implies that for all $l \in [\![1,k]\!]$, the set $\{a_l + 1, \ldots, b_l\} \cap \{b_1, \ldots, b_{l-1}\}$ is empty. Thus,

$$b_l = \min\left([\![i_l + 1, n]\!] \cap (\{b_1, \ldots, b_{k+1}\} \setminus \{b_{l+1}, \ldots, b_k\})\right),$$

so that $\Pi((a_1, \ldots, a_k), \{b_1, \ldots, b_{k+1}\}) = (b_1, \ldots, b_k)$. Moreover, the residue of this parking process is $b_{k+1} = 1$. It follows from the definition of $\Gamma_{n,k}$ that $\Gamma_{n,k}((i_1, \ldots, i_k), \{b_1, \ldots, b_{k+1}\}) = \gamma$.

The definition of $\Gamma_{n,k}(A,B)$ shows that it is actually a function of $(1 \ldots n)^{1-\rho(A,B)}A$ and $(1 \ldots n)^{1-\rho(A,B)}B$. This observation and the first assertion of Lemma 5.1 imply that $\Gamma_{n,k}$ is invariant under the shift modulo n.

Let us finally prove that each fibre of $\Gamma_{n,k}$ consists in one single orbit of the shift. Let $(A,B) \in [\![1,n]\!]^k \times \binom{[\![1,n]\!]}{k+1}$ be such that $\rho(A,B) = 1$. Let σ be a permutation which reorders $P(\Gamma_{n,k}(A,B))$ into a non-decreasing sequence and write $\sigma \cdot \Gamma_{n,k}(A,B) = ((i_1\, j_1), \ldots, (i_k\, j_k))$. Then $A = \tilde{A} = P(\Gamma_{n,k}(A,B))$ and $B = \tilde{B} = \{1, j_1, \ldots, j_k\}$. Hence, each fibre of $\Gamma_{n,k}$ contains a unique pair (A,B) such that $\rho(A,B) = 1$.

To be complete, one should conclude by observing that the action of $\mathbb{Z}/n\mathbb{Z}$ on $[\![1,n]\!]^k \times \binom{[\![1,n]\!]}{k+1}$ is free. □

Acknowledgement. It is a pleasure to thank Philippe Marchal who brought parking functions and their relation to the enumeration of minimal factorisations to my attention.

References

[1] Emil Artin. Theory of braids. *Ann. of Math. (2)*, 48:101–126, 1947.

[2] Philippe Biane. Minimal factorizations of a cycle and central multiplicative functions on the infinite symmetric group. *J. Combin. Theory Ser. A*, 76(2):197–212, 1996.

[3] Thierry Lévy. Schur-Weyl duality and the heat kernel measure on the unitary group. *Adv. Math.*, 218(2):537–575, 2008.

[4] Vivien Ripoll. Orbites d'Hurwitz des factorisations primitives d'un élément de Coxeter. *J. Algebra*, 323(5):1432–1453, 2010.

[5] Richard P. Stanley. Parking functions and noncrossing partitions. *Electron. J. Combin.*, 4(2):Research Paper 20, approx. 14 pp. (electronic), 1997. The Wilf Festschrift (Philadelphia, PA, 1996).

Thierry Lévy
Université Pierre et Marie Curie - Laboratoire de Probabilités et Modèles Aléatoires
Case courrier 188 - 4, place Jussieu - F-75252 Paris Cedex 05
`http://www.proba.jussieu.fr/pageperso/levy/index.html`